REMARKS

This Amendment responds to the final office action dated January 29, 2007. Reconsideration is respectfully requested.

A) Interview Summary

A telephone interview between the applicant, the applicant's representatives, and Examiner Tesolovich was conducted on July 18, 2007. The purpose of the interview was to discuss the section 112 rejections in the final office action, and in particular the use of the phrase "ephemeral key pair" in all of the claims. During the interview, the applicant and applicant's representatives re-stated their position that the use of this phrase in the claims is consistent with the common usage of the term in the field. In particular, the phrase "ephemeral key pair" is meant to refer to a key pair that is of limited temporal duration, *i.e.*, a temporary key pair that is used for a single message transaction only, as distinguished from a long term key pair, such as the key pair used in the certification stage of the public key encryption process, which may be used for multiple message transactions over a long period of time. Applicant and his representatives explained that by distinction the claimed "ephemeral key pair" is used in the encryption and digital signature phases of the public key process, which generate a different ephemeral key pair for each message transaction. Thus, the claimed "ephemeral key pair" is used for a single message only, and thereafter it is destroyed or deleted.

Examiner Tesolovich further explained her position regarding the section 112 rejections, and indicated that the 112 rejections may be overcome if the claims were clarified to indicate the extent or duration in which the ephemeral key pair was being used. In addition, Examiner Teslovich indicated that if the section 112 rejections were overcome, then the 102 rejections over Schneier would be moot.

B) Rejections under 35 U.S.C. § 102

Claims 1-45 were rejected under 35 U.S.C. § 102(e) as being anticipated by Schneier (U.S. Pat. 5,956,404). In the final office action, however, the Examiner indicated that "applicant's arguments with respect to Schneier's failure to specifically disclose the two part use of an ephemeral key pair are in fact persuasive." The Examiner nevertheless maintained the 102 rejections due to the section 112 issues discussed below. Applicant maintains that in view of the claim amendments and remarks set forth herein, the section 112 rejections have now been overcome, and thus the 102 rejection over Schneier should be withdrawn.

C) Rejections under 35 U.S.C. § 112

The independent claims have now been amended to further clarify the extent and duration of use of the claimed "ephemeral key pair," per the Examiner's suggestion. Specifically, the claims have been amended consistent with the specification and drawing figures to show that for each message transaction between a sender and a receiver the "ephemeral key pair" is produced and used to encrypt and digitally sign the particular plaintext message being communicated. Thus, the claims have been clarified to indicate that the ephemeral key pair is used for a single message transaction, and therefore the section 112 indefiniteness rejection should be withdrawn.

The dual use of such a per-message ephemeral key pair is clearly supported by the specification, and one of skill in the art would be enabled to practice the claimed invention in view of at least the following explicit support thereof. Page4, lines 6-9 of the specification, for example, state "in the present invention, there is provided an improved encryption and digital signature scheme ***that reuses an ephemeral key pair from the encryption process in the signature process***. Advantageously, the reuse of the ephemeral key allows the digital signature to be reduced in byte size." (emphasis supplied) In addition, page 5, lines 7-9 state "the

improved digital signature scheme uses the value of x, an encryption ephemeral key, for the value of z, a signature ephemeral key, instead of generating a random value for z, as in the prior art." Moreover, the problems in the prior art method of generating two separate ephemeral key pairs, one for the encryption phase and a second for the digital signature phase, are highlighted at page 9, lines 5-9 of the specification as follows "[F]irstly, computational resources and time consumed where Z is calculated with large bit numbers. Secondly, the byte-size overhead associated with the public-key transmitted information is undesirably large for bandwidth sensitive devices such as wireless communication devices."

Figure 4 of the present application, set forth below, clearly demonstrates the dual-use sharing of the temporary ephemeral key pair in the message encryption and digital signature phases of a public key encryption process. In Figure 4, the encryption ephemeral key pair (x, X) is generated in the encryption phase 16, which generates a ciphertext message using this temporary key pair. Then, in the digital signature phase 32, instead of generating another temporary key pair for the digital signature process, the ephemeral key pair (x, X) from the encryption phase is re-used in the digital signature phase by setting z to x and Z to X.

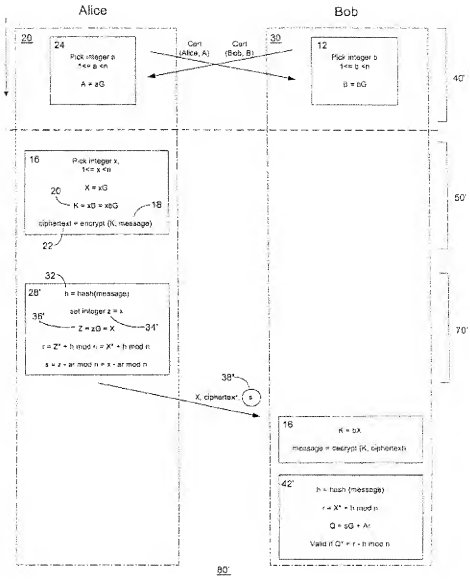

FIG. 4

This "dual use" of an ephemeral key pair in the encryption and digital signature phases of the public key encryption process, and the advantages thereof, is described in the specification as follows:

> "The improved digital signature scheme of the present invention uses the encryption ephemeral key pair (X, x) produced in the encryption stage 50' as a substitute for the signature ephemeral key pair (Z, z) required in the digital signature stage 70'. The value of signature ephemeral private key z

> 34' is set to the value of encryption ephemeral private key x from the encryption stage. Consequently, the random generation of z and the computation of Z 36' are not required since signature ephemeral public key Z 36' equals encryption ephemeral public key X 20. Advantageously, this reduces the computational load on the sender. In essence, the value for x is used for two different purposes. In the first instance, x is used for the encryption process scheme 50'. In the second instance, the x is also used in the digital signature scheme 70'." (Specification, page 9, line 23 through page 10, line 6.)

Based on this explicit disclosure in the specification, applicant maintains that there is adequate support in the application for the dual use of an ephemeral key pair, and thus the section 112 enablement rejection should be withdrawn.

This application is in condition for allowance.

Respectfully submitted:

David B. Cochran

JONES DAY
David B. Cochran
Reg. No. 39,142
901 Lakeside Ave.
Cleveland Ohio, 44114
216-586-7029
dcochran@jonesday.com